Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

PRIVACY AND SECURITY ISSUES IN INTERNET OF THINGS

Sarika Chaudhary

Assistant Professor, Dept. of CSE/IT, Amity School of Engineering & Technology, Amity University, Haryana, India.

ABSTRACT

Internet of Things (IoT) are all over in our daily life. They're utilized in our homes, in hospitals, deployed outside to control and report the changes in setting, forestall fires, and much more helpful practicality. However, all those advantages can return of a large number of risks including privacy loss and security problems. To secure the IoT devices, several analysis works are conducted to step those issues and realize an improved thanks to eliminate those risks, or at least minimize their effects on the user's privacy and security requirements. In the first section IoT devices are discussed. The second one will present IoT device limitations and in third section the classification of attacks on IoT are discussed. The last section can focus on the security of IoT in different layers.

KEYWORDS: Attacks, Internet of things, Privacy, Risk, Security.

Introduction

Internet of things (IoT) could be a assortment of "things" embedded with physical science, software, sensors, actuators, and connected via the net to gather and exchange information with one another. The IoT devices area unit equipped with sensors and process power that change them to be deployed in several environments. A range of common IoT applications is a good home, smart city, good grids, medical and aid instrumentation, connected vehicles, etc. The quick growth of the amount of IoT devices utilised is predicted to achieve forty one billion in 2020 with Associate in Nursing $8.9 trillion market [1] as expressed within the 2013 report of the International Data Corporation (IDC). The distinction between IoT and also the traditional web is that the absence of Human role. The IoT devices will produce info regarding individual's behaviors, analyze it, and take action [2]. Services provided by IoT applications supply an excellent profit for human's life, but they can keep company with an enormous value considering the person's privacy and security protection.

Security and privacy stay brobdingnagian problems for IoT devices, which introduce a full new degree of on-line privacy issues for customers. That's as a result of these devices not solely collect personal info like users' names and phone numbers, however may also monitor user activities (e.g., when users are in their homes and what that they had for lunch). Following the never-ending string of disclosures concerning major knowledge breaches, consumers square measure cautious of inserting an excessive amount of personal knowledge in public or personal clouds, with sensible reason.[3]

In this survey paper, the IoT security and privacy issues in four aspects are explored. The primary half presents the foremost relevant limitations of IoT devices and their solutions. The second half discusses the classification of existing IoT attacks. Then, we explore the IoT authentication and access management schemes and architectures projected in recent literature. Finally, we analyze the protection problems and mechanisms within the perception layer, network layer, transport layer, and application layer, respectively.

IoT Device limitation

Trappe et al. [9] presented the issue of IoT constraints, and their effects on using current cryptographic tools as the ones utilized in traditional Internet. The two main limitations are the battery capacity and computing power.

Battery Life Extension:

As some IoT devices area unit deployed in environments where charging isn't accessible, they solely have a restricted energy to execute the designed practicality and serious security instructions will drain the devices resources. [4] attainable approaches are often accustomed mitigate this issue. The primary is to use the minimum security needs on the device, which is not counseled particularly once handling sensitive data. The second approach is to extend the battery capability. However, most IoT devices area unit designed to be light-weight and in tiny size. There's no additional area for a bigger battery. The final approach is to reap energy from natural resources (e.g., light, heat, vibration, wind), however this sort of approach would require Associate in Nursing upgrade to the hardware and considerably increase the financial value[5].

light-weight Computation:

The paper [9] mentioned that standard cryptography cannot work on IoT systems, since the devices have restricted memory area that can't handle the computing and storage requirements of advanced cryptography algorithms. To support security mechanisms for the strained devices, the authors suggested reusing existing functions. A specific analog characteristics of a transmitter are often accustomed effectively inscribe analog info. These analog nuances can't be foreseen or controlled in producing, and can serve as a novel key. This manner of authentication has very little or no energy overhead as a result of it takes advantage of radio signals.

Attacks on IoT

Andrea et al. [12] come up with a brand new classification of IoT devices attacks given in four distinct types: physical, network, software, and coding attacks. Every one covers a layer of the IoT structure (physical, network, and application), in addition to the IoT protocols for encryption. The physical attack is performed once the attacker is during a shut distance of the device. The network attacks contain manipulating the IoT network system to cause damage. The software attacks happen once the IoT applications present some security vulnerabilities that permit the attacker to seize the chance and damage the system. Cryptographic attacks contains breaking the system encryption. This sort of attacks is often done by facet channel, cryptography, and man-in-the-middle attacks. Supported the study, to measure the security issues at the physical layer, the device has to use secure booting by applying a cryptological hash algorithms and digital signature to verify its authentication and the integrity of the software package. At the network layer, authentication mechanisms and point-to-point encryption are often wont to guarantee information privacy and development security. The application layer may give security by means of authentication, encryption, and integrity verification, which permits solely the approved users to access information through control lists and firewalls, additionally to the employment of antivirus software.

Ronen et al. [11] introduced a brand new taxonomy classification for IoT attacks supported however the attacker options deviates from the legitimate IoT devices. The classification are given in: ignoring, reducing, misusing, and increasing the system functionality. The study targeted on the practicality extension attacks on sensible lights. In this paper two attacks are presented: the first one consisted of making a covert channel to capture confidential information from a corporation building that implemented sensible lights which are connected to the interior sensitive network. The work is completed by exploitation an optical receiver that would scan the info from a distance of over a hundred meters by measurement the precise length and frequency of the small changes within the lights intensity. The second attack showed that an attacker will use those lights to form strobes within the sensitive lightweight frequencies, which may cause a risk of epileptic seizures. The experiments showed that it's necessary to focus on security problems throughout the various phases of planning, implementing and desegregation of the IoT devices.

IoT Security

Applying existing net standards to sensible devices will simplify the combination of the unreal situations within the IoT contexts. However, the protection mechanisms in typical Internet protocols got to be changed or extended to support the IoT applications. In this section, we tend to discuss the protection problems and existing solutions in numerous layers of IoT.

IoT Perception Layer Security:

IoT system is intended to gather and exchange knowledge from the physical world. Hence, the perception layer contains numerous types of aggregation and dominant modules, like the temperature sensors, sound sensors, vibration sen-

sors, pressure sensors, etc. The perception layer will be more divided into two parts: perception node (sensors or controllers, etc.), perception network that communicates with transportation network [6]. Perception node is employed for knowledge acquisition and knowledge management, perception network sends collected knowledge to the gateway or sends control instruction to the controller. Perception layer technologies embody wireless sensing element networks (WSNs), implantable medical devices (IMDs), Radio- Frequency IDentification (RFID), world Positioning System (GPS), etc. One perception layer security issue is that the detection of the abnormal sensor node. This might happen once the node is physically attacked (e.g. destroyed, disabled), or intruded/compromised by cyber-attacks. These nodes are named as faulty nodes generally. So as to make sure the standard of service, it is necessary to be ready to observe the faulty nodes and take actions to avoid additional degradation of the service.

IoT Network Layer Security:

For IoT devices in WSN context, it's fascinating to increase IPv6 over Low power Wireless Personal space Networks (6LoWPAN) to change IPSec communication with IPv6 nodes. This is helpful as a result of the prevailing end-points on the Internet don't ought to be changed to speak firmly with the WSN, and therefore the true end-to-end security is enforced without the requirement for a trustworthy entryway. Raza et al. [10] proposed AN End-to-End (E2E) secure communication between IP enabled sensing element networks and therefore the ancient web. Their extension of LoWPAN supports each IPSec's Authentication Header (AH) and Encapsulation Security Payload (ESP), so that the communication endpoints are able to evidence, encrypt and check the integrity of messages by making use of standardized and established IPv6 mechanisms.

IoT Transport Layer Security:

Brachmann et al. [7] pointed out that security protocols such as Transport Layer Security (TLS) or DTLS adopted on the Internet doesn't essentially mean that an equivalent security levels is achieved in Low-power and lossy Network (LLN), that continues to be liable to resource exhaustion, flooding, replay and amplification attacks, since the 6LoWPAN Border Router generally doesn't perform any authentication. The authors bestowed two approaches to mitigate such attacks. The first is to map the TLS to DTLS protocol to make sure end to- end security at the appliance layer. The second approach is to use DTLS-DTLS tunnel to shield the LLN.

IoT Application Layer Security:

IoT features a wide range of applications, together with however not limited to sensible home (e.g., learning thermostat, sensible bulb), medical and attention (e.g., time period health observation system), smart town (e.g., sensible lighting, sensible parking), energy management (e.g., sensible grids, sensible metering), environmental monitoring (e.g., climate observation, life tracking), industrial internet, connected vehicle Most modern IoT devices contain configurable embedded computer systems. Some area unit even running advanced code and resembling all-purpose computers, hence they face the same security risks as that of all-purpose computers. When connected to the net, they might get infected by computer virus like trojan. The net of Things (IoT) is making a brand new surroundings where malware are often wont to produce powerful botnets. Mirai [8], a recently discovered piece of UNIX operating system malware, is being employed to rope IoT devices into botnets. Mirai will gain shell access using the default countersign of the telnet or SSH accounts. After it obtains access to the account, it will produce delayed processes, delete files, and even install alternative malware on the system. The infected devices were on the QT below Mirai's control and awaiting orders to strike within the sort of DDoS attack. The Brobdingnagian web outage in Oct 2016 was caused by the DDoS attack exploitation compromised IoT devices running the Mirai malware.

Conclusions:

In this survey, various the security and privacy issues in IoT applications and systems are presented. The limitations of IoT devices in battery and computing resources are pointed out, and discussed possible solutions for battery life extension and lightweight computing. Also approaches for IoT attacks and security mechanisms are mentioned. The last part of paper analyzed the safety problems and solutions in four layers, together with the perception layer, network layer, transport layer, and application layer. Overall, the protection of economic IoT devices nowadays depends on the technologies, protocols, and security mechanisms enforced by every individual manufacturer. Supported the precise case, all IoT devices might be at risk of sure styles of attacks. IoT producing business must work closely with the superordinate agencies, like FSA and DHS, and also the standardization organizations to tackle recently emerged threats on develop robust and sturdy security standards for IoT devices and systems.

REFERENCES

1. IoT Analytics, "Why the internet of things is called internet of things: Definition, history, disambiguation," https://iot-analytics.com/internetof-things-definition/, 2014.
2. Saif,I., Peasley,S., and Perinkolam,A., "Safeguarding the internet of things: Being secure, vigilant, and resilient in the connected age," https://dupress.deloitte.com/dup-us- en/deloittereview/issue-17/internet-of-things-data-security-and-privacy.html, 2015.
3. Talkin Cloud, "Iot past and present: The history of iot, and where it's headed today," http://talkincloud.com/cloud-computing/iot-past-andpresent-history-iot-and-where-its-headed-today?page=2, 2016.
4. Rouse,M., "Iot security (internet of things security)," http://internetofthingsagenda.techtarget.com/definition/IoT-security- Internet-of-Things-security, 2013.
5. Trappe,W., Howard,R., and Moore, R.S.,"Low-energy security: Limits and opportunities in the internet of things," IEEE Security Privacy, vol. 13, no. 1, pp. 14–21, Jan 2015.
6. Jing,Q., Vasilakos,A.V., and Qiu,D. "Security of the internet of things: perspectives and chenges," Wireless Networks,vol. 20, no. 8, pp. 2481–2501, 2014.
7. Brachmann,M., Keoh,S.L., Morchon,O.G., and S. S. Kumar, "End-to end transport security in the ip-based internet of things," in 2012 21st International Conference on Computer Communications and Networks (ICCCN), July 2012, pp. 1–5.
8. Wikipedia, "Mirai," https://en.wikipedia.org/wiki/Mirai_(malware), 2016.
9. Hummen,R., Ziegeldorf,J.H, Shafagh,H., Raza,S. and Wehrle,K., "Towards viable certificate-based authentication for the internet of things," in Proceedings of the 2Nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy, ser. Hot WiSec '13, 2013, pp. 37–42.
10. Raza,S., Trabalza,D. and Voigt,T. "6lowpan compressed dtls for coap," in 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, May 2012, pp. 287–289.
11. Ronen,E., and Shamir,A., "Extended functionality attacks on iot devices: The case of smart lights," in 2016 IEEE European Symposium on Security and Privacy (EuroS&P), March 2016, pp. 3–12.
12. Andrea,I., Chrysostomou,C., and Hadjichristofi,G., "Internet of things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015, pp. 180–187.